聚铭网络流量智能分析审计系统
产品白皮书

南京聚铭网络科技有限公司

2019 年 7 月

版权声明

南京聚铭网络科技有限公司（以下简称为聚铭网络、JUMING）。

JUMING 聚铭图标为南京聚铭网络科技有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系南京聚铭网络科技有限公司技术服务部。

联系信息

地　　址：南京市雨花区软件大道 180 号 07 栋 406 室

邮　　编：210000

电　　话：025-52205520 025-52205570

传　　真：025-52205565

邮　　箱：support@juminfo.com

网　　址：www.juminfo.com

全国客服电话：400-1158-400

目录

1. 前言

随着各类信息技术及软硬件系统的持续演进，信息安全问题日益严峻，而且我国当前信息系统安全产业及相关安全法律法规及其标准也不甚完善，这导致国内信息安全保障工作严重滞后于信息技术发展的速度。

由此，目前各企业 IT 系统信息安全面临巨大的困境，主要包括：

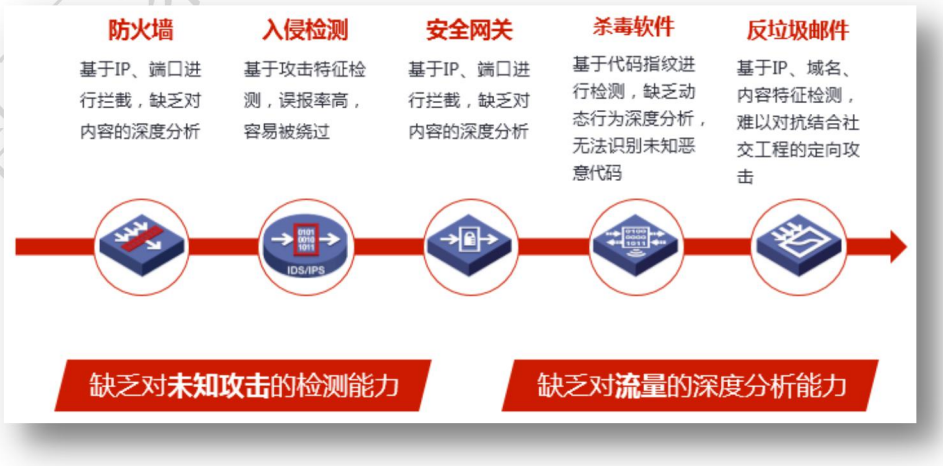
- 落后的边界隔离理念 VS 灵活多变的渗透技术
- 日益臃肿的攻击特征库 VS 专业智能的 SaaS 服务
- 一片祥和的监控页面 VS 暗流涌动的隐蔽信道

只重视边界的防护，而忽视内部系统安全问题的传统观念已经无法适应当前日益严峻的安全形势；没有安全事件和告警不等于没有被攻击者盯上和攻击。

企业虽然购置了大量安全设备及产品（防火墙、入侵检测、安全网关、杀毒软件、反垃圾邮件），但这些产品大都是基于已知规则库进行监测，可检测出已知安全威胁，如果数据被加密或者被做了免杀处理，则无能为力。

传统的安全设备无法保存全流量数据，在发现入侵行为后，无法做到完整的溯源取证和损失评估。

新型未知威胁的攻击手段越来越老练，在单个时间点无明显特征，隐蔽能力强，攻击渠道不确定，攻击空间路径不确定，长持续性，传统基于特征的分析手段难以发现和分析。



2. 客户需求

针对上述问题和挑战，一般企业的信息安全管理人员不仅对各类**安全合规**功能有着较高要求，而且对日常**安全问题的发现、潜在问题的萃取、未发生问题的预防等**都有较高期望，特别是对于一些**隐蔽安全问题的追根溯源**（包括各类高级持续威胁等）也有现实需求，包括：

1. 通过企业网站等途径的外部渗透行为；
2. 通过邮件钓鱼等途径的鱼叉攻击行为；
3. 访问控制混乱而导致的隐蔽通道或服务端口暴露问题；
4. 内部潜在威胁源或威胁用户的发现；
5. 潜在的数据泄露或外传风险；
6. 其它各类网络异常行为的检测。

以上仅列举了部分内容，但在现实中安全问题远远不止上述部分，例如还有针对各种 0day 漏洞的攻击等等，所以客户对网络流量分析审计的要求应包含了对于**未知威胁的检测和防御**，而不仅仅是对于**已知威胁**的发现。

3. 聚铭网络流量智能分析审计解决方案

聚铭网络流量智能分析审计系统（iNFA）是南京聚铭网络科技有限公司研发的具有自主知识产权的专业网络流量分析审计系统，它具有独特而强大的网络流量审计和分析功能，结合失陷分析、威胁情报分析、异常行为分析、未知威胁分析、网络异常分析、域名异常分析、攻击威胁特征分析、隐蔽通道分析以及丰富的整体安全分析报告功能，可有效检测外部攻击、外连威胁、内部非法连接、网络会话模式异常等安全威胁，是对传统安全防御系统的完善和补充，成为企业提升安全防御水平的有力武器和必要工具。同时，也是满足国家等保测评、网络安全法及行业安全规范的最佳解决方案。

3.1. 技术方案

聚铭网络流量智能分析审计系统包括流量采集、数据分析、攻击检测、文件检测、威胁情报检测、异常行为检测等六大处理引擎，通过对全流量进行采集和分析，有效保证用户终端的安全。

◆ 流量采集引擎

实现快速流量会话重建、协议模糊识别、元数据抽取等功能。

◆ 数据分析引擎

提供元数据搜索/分析、安全事件分析及审计、取证分析、数据挖掘功能。

◆ 攻击检测引擎

根据内置的近 40 余类、约两万余条攻击检测规则，对可疑的网络会话进行检测并可以下载相关原始数据包。

◆ 文件检测引擎

实现从 HTTP、邮件、SMB、FTP、QQ 等协议中还原文件，并对文件进行病毒扫描、敏感词检测，不仅能够发现恶意软件，还能够防止客户的核心数据外泄。

◆ 威胁情报检测引擎

集成动态域名、Spyware IP/Bot IP/ Spammer IP、被黑主机、扫描结点、C&C 回连结点、钓鱼 URL、虚假防病毒网站、TOR、VPN/Socket 代理等若干类的安全情报。

◆ 异常行为检测引擎

集成自主研发的大数据技术对流量特征分析、建模，智能生成该对象多维度的网络特征，实施多维度的纵深检测。

3.2. 主要功能

3.2.1. 威胁检测

通过对网络流量进行非入侵性的侦听检测，在威胁发生全生命周期的多个阶段识别攻击者的攻击负荷、恶意行为和网络通信。

3.2.1.1. 全流量采集深度包解析

采用零拷贝、全程无锁化技术处理网络流量数据包，而且充分利用 CPU 向量化指令对各类模式进行识别或匹配，故即使在超大流量情况下，也能保证系统整体处理无延时；独有的智能协议识别技术，可高速、准确地识别上千种应用，检测各种协议伪装行为；支持 HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet 等应用协议的精准解码、元数据提取及存储、搜索、统计功能，并对可疑网络流量进行了全包留存。

3.2.1.2. 攻击检测

内置多种网络攻击检测策略，支持对一般网络攻击、明文传输、过期系统或软件、木马检测、隐蔽通道、电子加密货币活动、勒索软件进行检测，支持检测的类型可达 34 种。

- ◆ 网络攻击检测：支持对一般的网络攻击进行检测，检测的类型包括端口扫描、拒绝服务攻击、漏洞利用攻击、SQL 注入攻击、缓冲区溢出攻击、Webshell 及其它类型的注入攻击；
- ◆ 明文传输检测：对网络传输中存在的明文传输行为进行检测；
- ◆ 过期系统或软件检测：支持对可能存在过期的系统或软件进行检测；
- ◆ 木马检测：支持对各类木马活动进行检测，包括但不限于木马软件下载、木马登录/回连以及其他木马通讯行为；
- ◆ 隐蔽通道检测：支持对各类隧道检测，对协议改写、安全洋葱等存在隐蔽通道的行为检测；

◆ 电子加密货币活动检测：支持对主流电子加密货币活动进行检测，包括但不限于比特币、莱特币、门罗币等；

◆ 勒索软件检测：支持对各类勒索软件进行检测，包括其登录行为、横向扩散行为等，检测的类型包括但不限于永恒之蓝、GandCrab、Satan 等。

3.2.1.3. 文件检测

3.2.1.3.1. 文件还原

支持从 HTTP、FTP、SMB、邮件、QQ 等应用协议中还原各类文件，支持 MS Office 文件、Mac Office 文件、HTML、Flash、RTF、PDF，以及 Zip、RAR、Dmg、Tar、Gizp、CHM、BinHex、SIS 等归档文件。

3.2.1.3.2. 文件静态扫描

对还原的文件进行加密检测、启发式扫描、威胁情报检测、数据泄密检测。

◆ 加密文件检测：支持对各类加密文件进行检测；

◆ 启发式扫描：支持对各类文件进行启发式扫描，检测威胁内容包含但不限于一般病毒、木马、蠕虫、各类灰件（含广告）、勒索软件等；

◆ 威胁情报检测：支持对各类文件进行恶意软件威胁情报匹配；

◆ 数据泄密检测：支持根据用户自定义的敏感词库，对各类传输文件进行扫描，检测内容中包含敏感词的文件，防止核心数据外泄。

3.2.1.3.3. 文件行为检测（需选配 UTA 引擎）

对于一些攻击者加花、加壳的恶意文件，可以轻易的绕过静态扫描检测，此时就必须要通过虚拟仿真环境运行文件，通过对文件的行为进行分析，从而判定其是否为恶意文件。

◆ 支持动态执行还原文件，文件行为分析，包括注册表、进程、网络、释放恶意文件等行为，支持提取攻击的完整样本，并提供样本的下载能力；支持检测 Word、Excel、PPT、PDF、EXE、DLL、ZIP、RAR、7z 等主流文件类型；

◆ 支持系统敏感操作、系统环境探测、反检测行为、反调试行为、木马回连、远控木马、网络通讯、勒索软件、恶意软件行为等文件恶意行为检测。

3.2.1.4. 威胁情报检测

整合威胁情报库，支持对各类恶意 IP、恶意域名、恶意 URL 以及恶意邮箱进行检测；检测的类型包括僵尸网络、木马回连、隐蔽通道、电子加密货币矿池等。

3.2.1.5. 网络质量检测

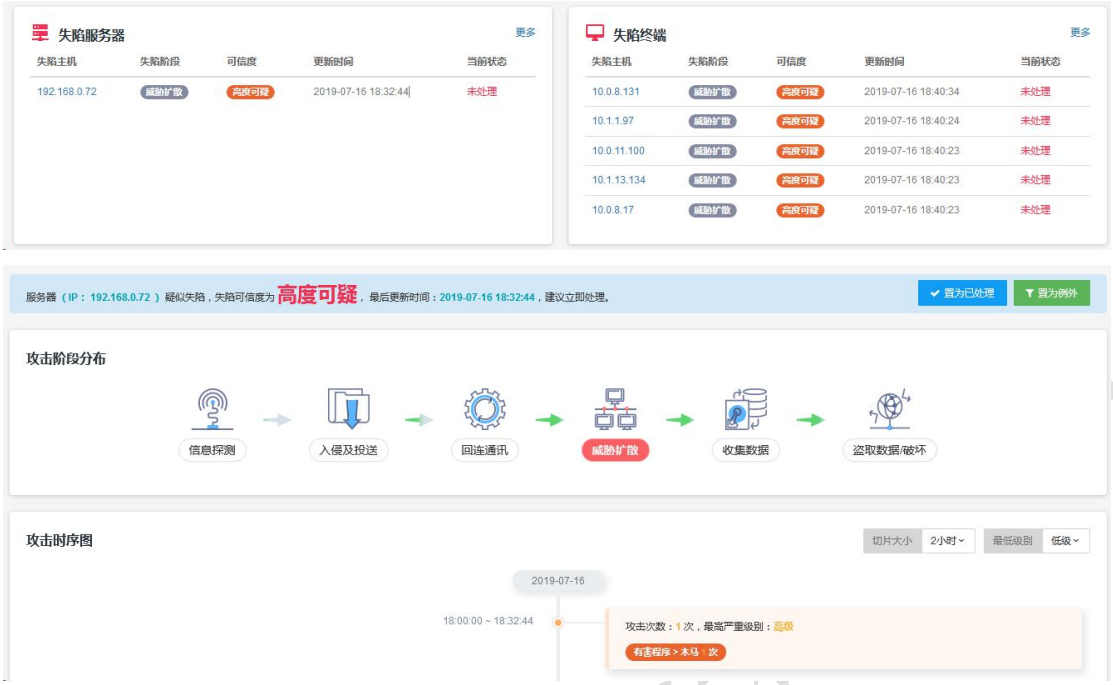
具备发现带宽占用异常、ARP 风暴、ICMP Flood、TCP 建连时延过长、TCP 重传过多、TCP 零窗口过多等网络质量异常的能力。

3.2.1.6. 异常行为检测

集成了聚铭网络自主研发的智能动态基线、模式信息熵等生成算法，通过一段时间对学习对象的流量特征分析、建模，智能生成该对象多维度的网络特征，实施多维度的纵深检测机制，增加检测的准确性，降低误报概率。

3.2.2. 失陷管理

在利用安全情报技术、大数据技术、AI 技术进行安全分析的基础上，结合 Kill-Chain 技术实时发现资产安全失陷情况，并支持分析溯源，详细展示各个失陷阶段的具体安全事件与原因；让运维人员摆脱海量安全事件、告警的困扰，聚焦问题所在，极大提升运维效率。



3.2.3. 威胁管理

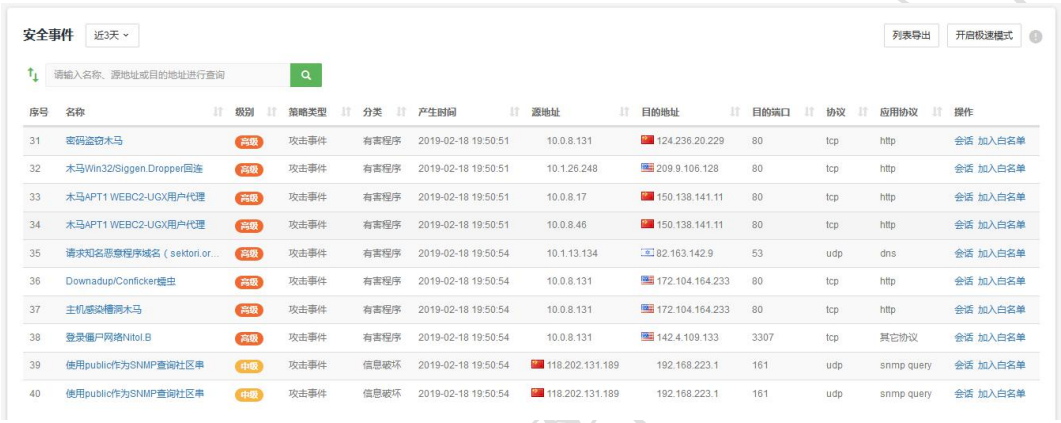
根据产生的安全事件，抽取用户需要关注的事件，并且可以通过安全事件页面对此类安全事件进行分析。用户可以将生成的报表通过定时发送邮件的方式汇报历史以来的威胁状况。

3.2.3.1. 重点关注事件

根据安全事件的影响程度和影响范围分级（极度、重点、中等、一般）呈现所有受害主机，并通过安全知识库指导用户了解相关威胁的原理和解决方案。

3.2.3.2. 安全事件分析

提供事件名称、严重级别、源地址、目的地址、源端口、目的端口、分类、子类（子类内容随分类联动）、协议类型、来源等全部或部分模糊查询，对安全事件对应的会话、攻击检测特征、网络访问域名信息、C&C 回连信息、动态算法生成域名（Dynamic Generating Algorithm，即 DGA）等通过多视图展示，全方位快速展示攻击或网络异常事件背后的信息。



3.2.3.3. 智能分析报告

提供事件名称、严重级别、源地址、目的地址、源端口、目的端口、分类、子类（子类内容随分类联动）、协议类型、来源等全部或部分模糊查询，对安全事件对应的会话、攻击检测特征、网络访问域名信息、C&C 回连信息、动态算法生成域名（Dynamic Generating Algorithm，即 DGA）等通过多视图展示，全方位快速展示攻击或网络异常事件背后的信息。

NFA 网络流量智能分析审计系统 | 总体分析报告 2019-07-23

第一章 概述

通过对各项数据的分析，发现当前系统 **26** 台主机存在安全问题或隐患；以下数据分别以连接方向阐述相关问题。

网络连接方式分别为外部主机或系统连接内部主机或系统、内部主机或系统连接外部主机或系统、内部主机或系统互相连接，存在安全的问题分别被称作外部威胁、外连威胁及内部互连威胁。

当前系统各类威胁具体如下：

外部威胁列表

序号	内网主机IP	类型	威胁数量
1	10.0.0.104	外部攻击	5339
2	10.0.0.104	口令猜测	5339
3	10.0.0.21	外部攻击	4866
4	10.0.0.21	口令猜测	4218
5	10.0.0.42	扫描探测	1400

显示 1 至 5 条记录，共 14 条记录 < 1 2 3 >

NFA 网络流量智能分析审计系统 | 安全事件报告 2019-07-23

第一章 概述

通过对各项数据的分析，当前系统共发现 **26** 种安全事件可能需要引起关注，**31** 台主机可能存在威胁。

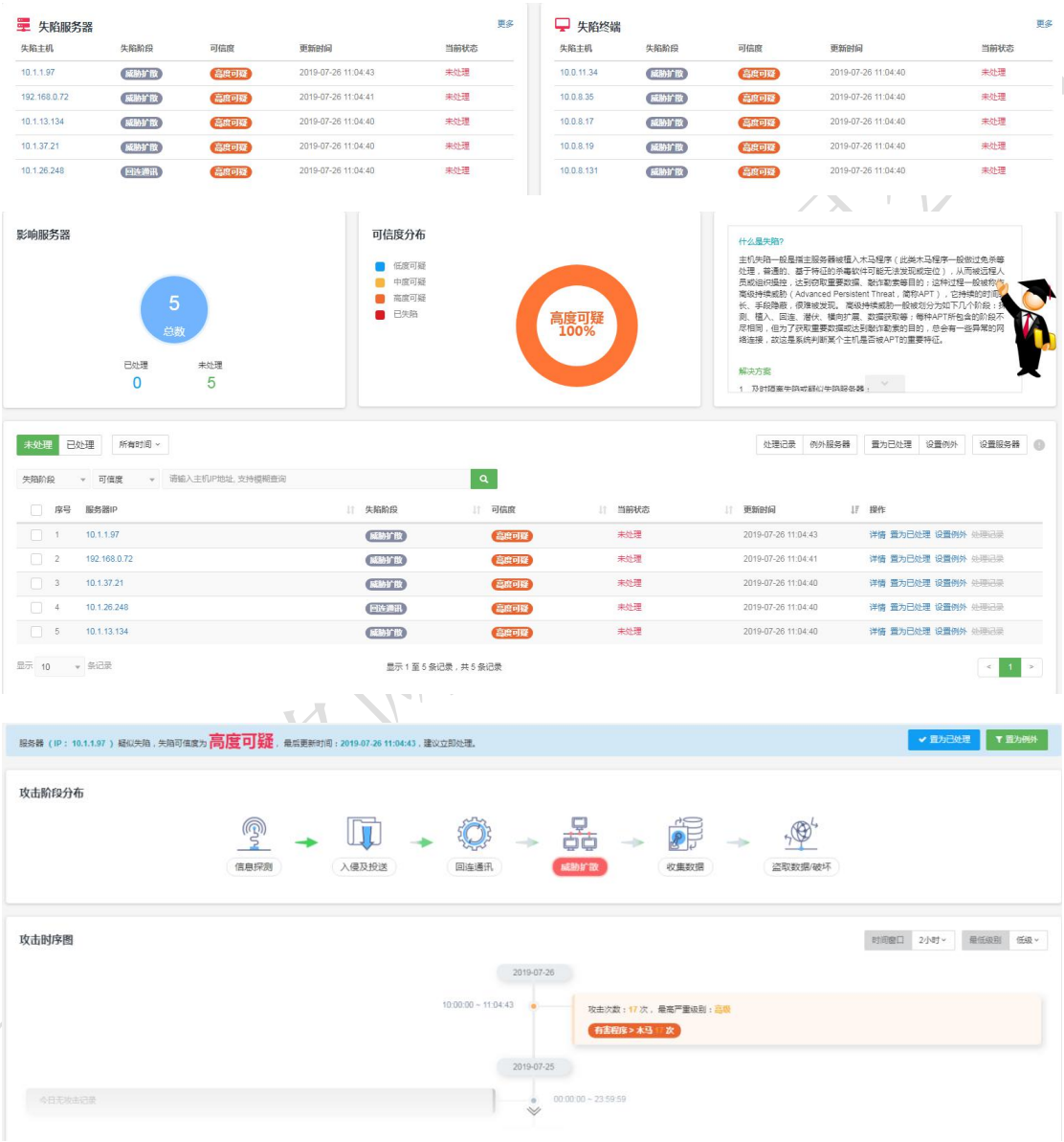
当前系统需要关注的安全事件具体如下：

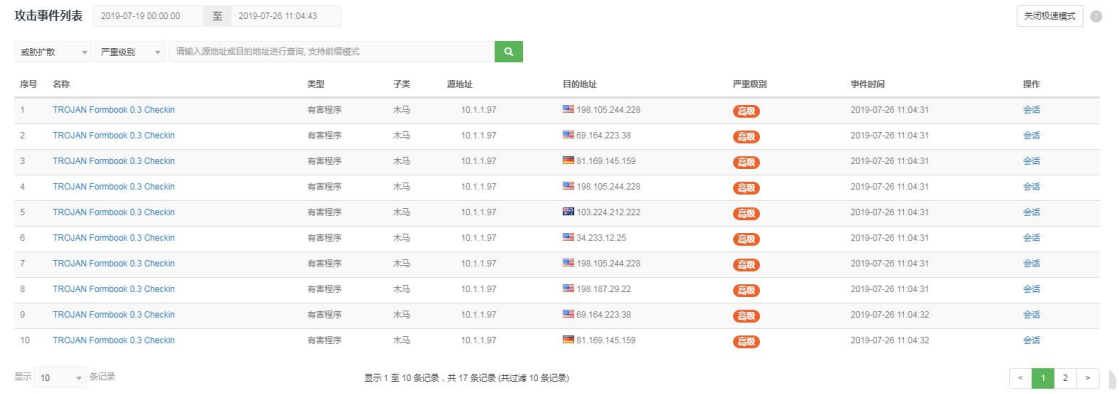
序号	名称	关注种类	关注程度	受害主机数量	描述	解决方案
1	永恒之蓝	勒索	极度	1	利用MS2017-010漏洞...	建议及时隔离相关主机...
2	Gapz木马	木马活动	重点	2	这是一个木马，它在受...	关闭电脑共享功能，关...
3	僵尸网络（Botnet）	僵尸网络	重点	2	用户计算已沦陷为"肉鸡...	及时调查可能失陷主机...
4	木马回连	木马活动	重点	2	失陷主机向远程控制端...	及时调查可能失陷主机...
5	缓冲区溢出攻击	服务器漏洞利用	重点	1	缓冲区溢出攻击是利用...	根据攻击的类型修补相...
6	Ramnit木马	木马活动	重点	1	通过移动介质传播的密...	及时隔离相关源主机，...
7	Downadup/Conficker木马	木马活动	重点	1	这是一种远控木马（蠕...	可以使用专用查杀软件...

3.2.4. 态势感知

3.2.4.1. 失陷态势感知

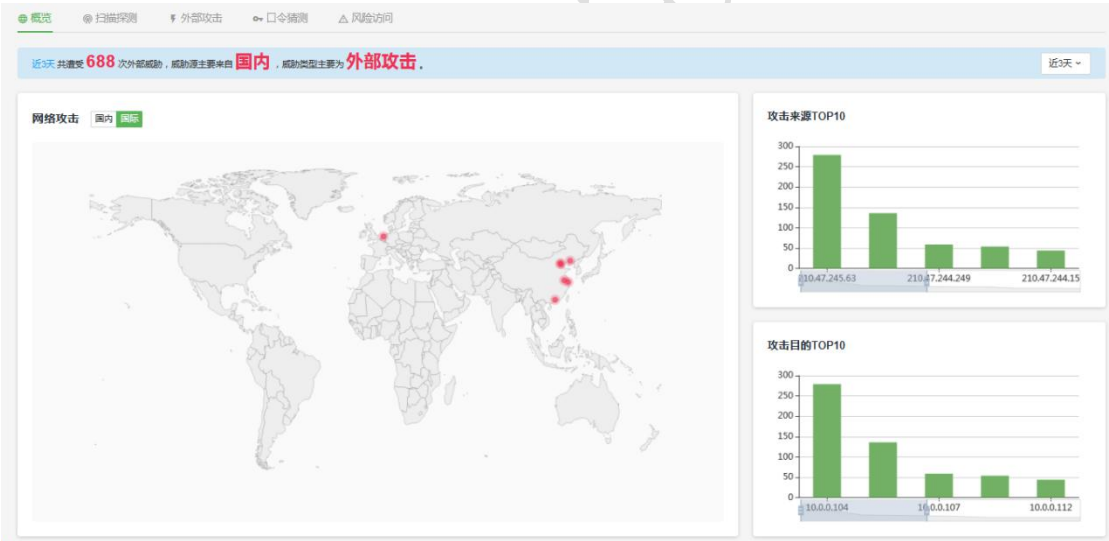
对服务器失陷/终端失陷进行监控。监控服务器失陷/终端的失陷阶段、判断失陷可信度、对历史失陷过程进行记录追踪。

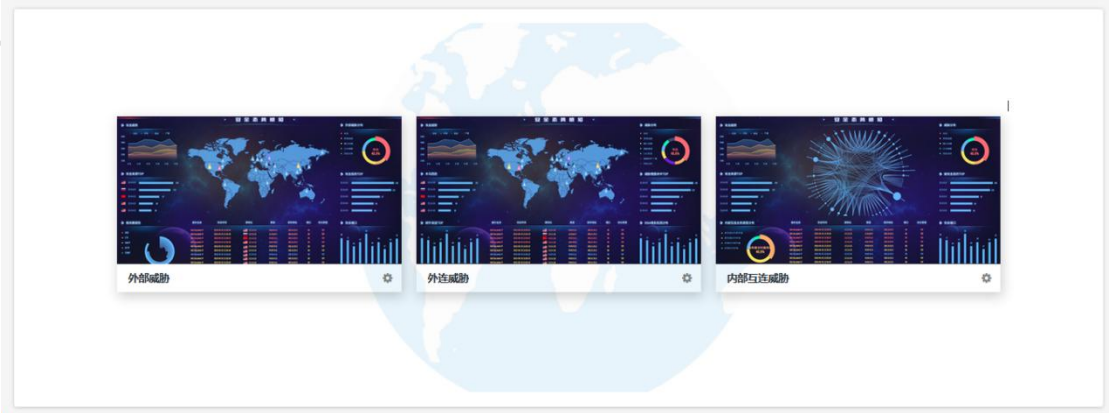




3.2.4.2. 网络威胁态势感知

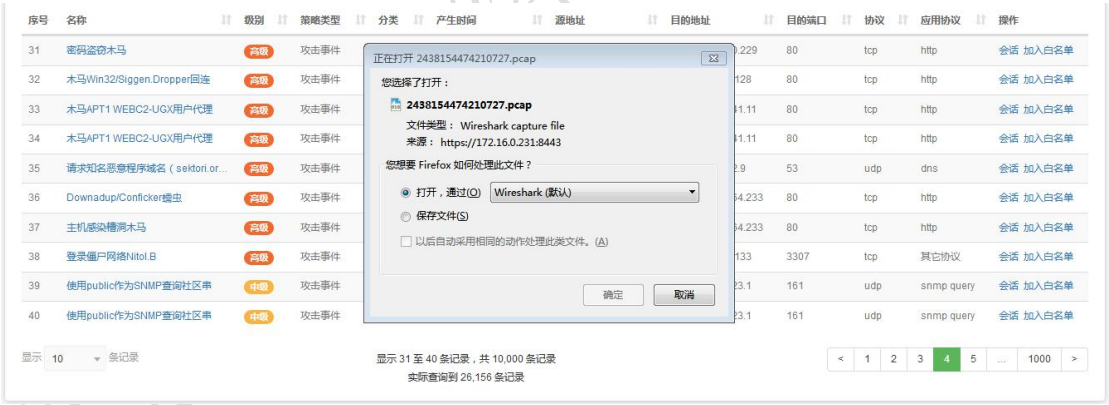
综合外部威胁、外连威胁、内部互连威胁三个方向全面监控网络威胁态势感知情况，关注扫描探测、外部攻击、口令猜测、风险访问、C&C 回连、隐蔽通道、恶意程序活动等网络威胁行为，并支持大屏投放监控。





3.2.5. 溯源分析

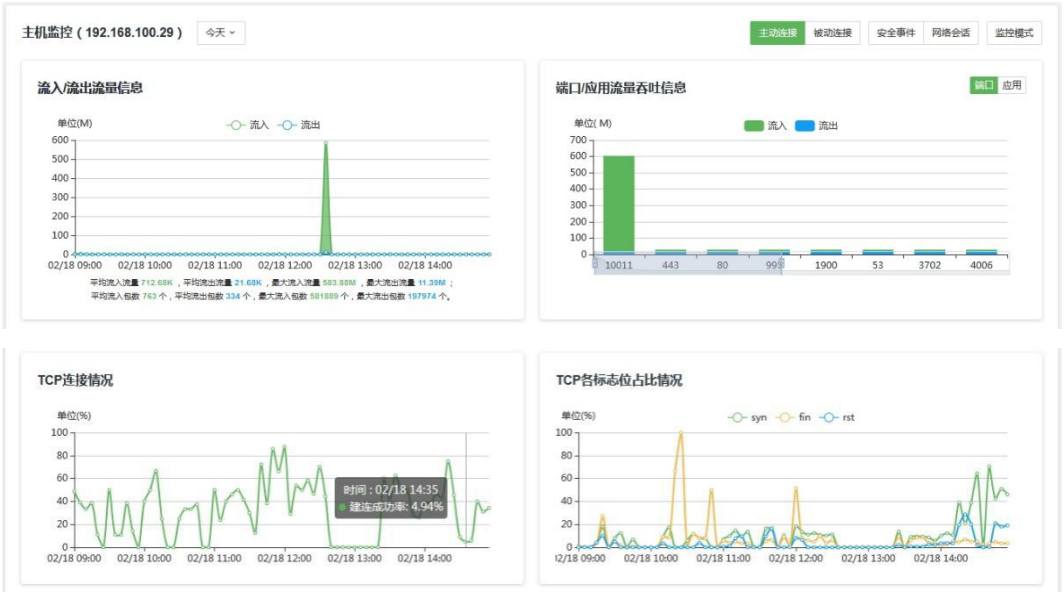
基于大数据检索技术，可快速的针对受害主机进行溯源分析，还原入侵行为的全过程，溯源粒度精确到会话数据包级别。



3.2.6. 性能监控

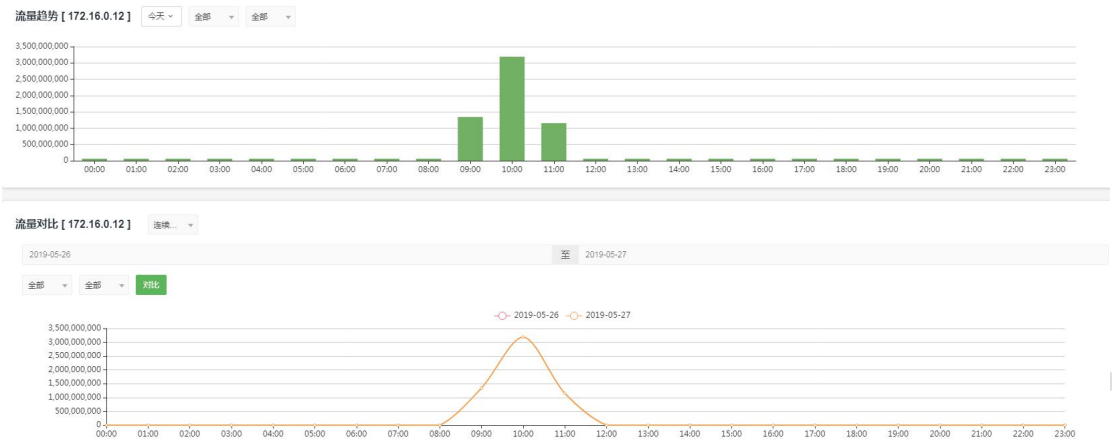
3.2.6.1. 主机性能监控

支持主机网络性能实时监控，以图表的形式监控主机的带宽占用情况、端口/应用的流量吞吐、TCP 建连成功率、TCP 三次握手时延、TCP 重传以及 TCP 零窗口等，并且支持查询模式回溯历史时间的网络质量情况。



3.2.6.2. 流量统计分析

支持实时统计流量使用情况，可通过列表查看每个主机的流入流量、流出流量，总流量，也可以通过配置交换机接口来监控各个网段的流入流量、流出流量、总流量。并且可通过下钻单个主机或网段，查询主机或网段的流量趋势，以及进行对比各个时间段的流量情况。



3.2.7. 会话审计

聚铭网络流量智能分析审计系统利用独有的智能协议识别技术，可高速、准确地识别上千种应用，在解析五元组（源 IP、目的 IP、源端口、目的端口、协议）、会话发生时间外，根据不同应用协议进行了更加深度的解析，满足客户会话审计的需求。

3.2.7.1. HTTP 会话审计

从流量中还原 HTTP 会话数据，并根据会话特征进一步深度解析 HTTP BBS 访问、HTTP 网页标题、HTTP 威胁情报、HTTP DGA 域名、搜索关键词及其他 HTTP 会话等，数据中至少包含请求方法、返回值、主机名、网页地址、用户代理、语言、服务器类型等数据。

3.2.7.2. DNS 会话审计

从流量中还原 DNS 会话数据，并根据会话特征进一步深度解析 DNS 威胁情报、DNS DGA 域名、DNS 解码错误、DNS 解析错误、DNS 解析超时，数据中至少包含请求域名（FQDN）、DNS 服务器地址、DNS 服务器端口、请求返回解析地址等信息。

3.2.7.3. FTP 会话审计

从流量中还原 FTP 会话数据，数据中至少包含登录用户、传输文件名以及**操作命令**等信息。

3.2.7.4. Telnet 会话审计

从流量中还原 Telnet 会话数据，数据中至少包含登录用户以及**操作命令**等信息。

3.2.7.5. 数据库会话审计

从流量中还原主流数据库会话数据，如 Mysql、SQLServer、Oracle、DB2、Sybase 等主流数据库，数据中至少应包含登录用户名、**操作命令（SQL）**等信息。

3.2.7.6. 邮件会话审计

从流量中还原邮件会话数据，包括 POP3，SMTP、IMAP 协议，数据中至少包含收件人、发件人、主题、附件名称等信息。

3.2.7.7. TLS 会话审计

从流量中还原 TLS 会话数据，数据中至少包含服务器及客户端证书、服务器名称等信息。

3.2.7.8. 其他会话审计

其他会话均通过可以网络会话菜单支撑审计，网络会话列表包含了全流量的会话还原留存，会话详情将根据不同的应用协议自动适配字段展现。

3.2.7.9. 工控会话

从流量中还原应用协议为 IEC、MMS、MODBUS、OPC、OPCUA、EthernetIIP CIP 的工控会话，数据中至少包含工控会话的 MODBUS 的功能码、功能描述，支持解析 IEC、 EthernetIIP CIP 的命令等信息。

3.3.用户价值

3.3.1. 网络威胁发现

聚铭网络流量智能分析审计系统具备强大的网络威胁发现能力，基于聚铭网络自主研发的威胁检测算法及开发的相关威胁特征库，确保及时、准确地发现各类网络安全问题。它不仅能检测外部攻击，同时也对内部威胁进行实时监控，只有抵御网络外部攻击的同时，揪出内部攻击的元凶，全网的安全才能得到保障，产品的双向检测功能无疑给用户网络提供了双重的安全保障。

3.3.2. 异常行为检测

聚铭网络流量智能分析审计系统集成了聚铭网络自主研发的智能动态基线、模式信息熵等生成算法。通过一段时间对学习对象的流量特征分析、建模，智能生成该对象多维度的网络特征，对于具有明显异常行为的对象进行告警。

3.3.3. 网络数据可视

聚铭网络流量智能分析审计系统通过对网络中的流量数据进行采集和分析，能够对全网状况进行实时监控，帮助网络管理员建立全网的视角，纵观网络的状况与趋势变化，及时掌控网络负载情况，以及网络应用资源的使用情况。

3.3.4. 网络数据留存

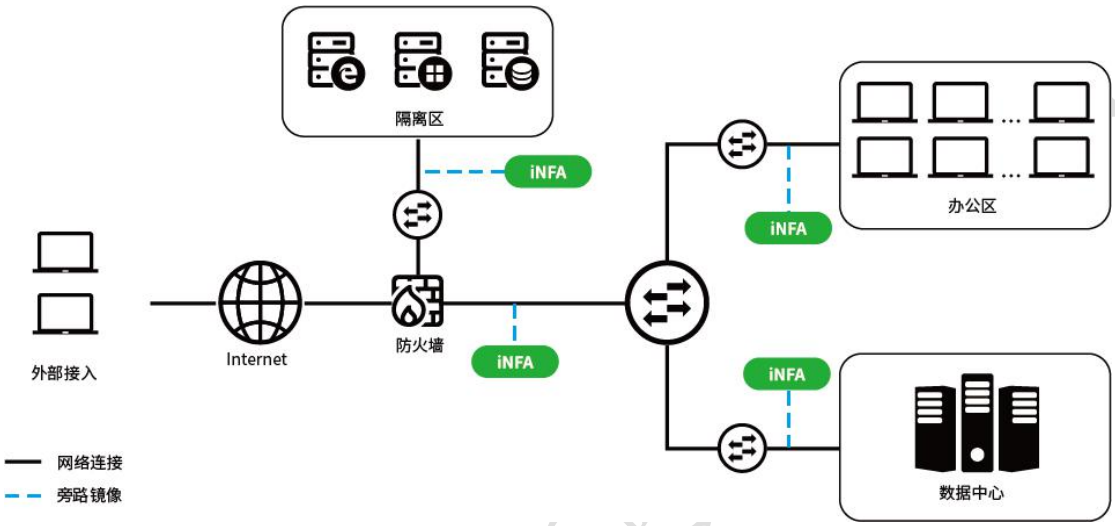
聚铭网络流量智能分析审计系统可高速地、实时地、不间断地保存各类网络会话元数据，并且它可以按应用协议类型留存各类原始网络数据包，为用户对网络相关问题进行调查和取证提供便利。

3.3.5. 网络审计合规

使用聚铭网络流量智能分析审计系统可满足如等级保护 2.0、《中华人民共和国网络安全法》等法律、法规对于网络数据审计的要求。

3.4. 部署方案

聚铭网络流量智能分析审计系统采用旁路 SPAN 部署方式和 TAP 部署方式，两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响；设备部署的示意图如下：



4. 南京聚铭网络科技有限公司简介

南京聚铭网络科技有限公司(Nanjing Juming Network technology Co.,Ltd)，是国内领先的安全产品提供商和安全运营商、**“双软企业”**、**“高新技术企业”**、**“江苏省民营科技企业”**、**“创业南京” 高层次创业人才企业**，服务于“能源、电信、教育、金融、政府、军工、医疗、公安”等多个行业。公司通过了 **ISO9001、ISO20000、ISO27001** 等众多的标准体系认证，**“聚铭综合日志分析系统”荣获江苏省软件产品金慧奖、南京市新兴产业重点推广应用的新产品，**公司始终秉承“真诚合作、互利共赢、优势共享，服务客户”的经营理念、先进的技术、优秀的产品和专业的配套服务，引领国内安全的发展方向。

为掌握核心科技，公司投入了大量的科研经费，先后成立了**“聚铭安全攻防实验室”**和**“智库评价和数据科学联合实验室”**两大科学研究和应用研究实验室。其中：“数据科学联合实验室”为本公司与南京大学中国智库研究和评价中心联合成立，专业从事于数据科学相关的理论研究和应用研究方向。“聚铭安全攻防实验室”专业从事于信息安全攻防应用研究方向。

公司现有团队超过一半以上的人员具有十年以上的安全产品研究、开发以及安全数据分析、运营、服务的经验；公司坚持技术自主创新，以产品服务为中心，以满足客户业务需求为目标，凭借多年的客户服务经验，构建了安全产品、安全运营、大数据分析平台及服务等系列产品和服务，以满足不同用户的需要。

未来，公司将继续致力于引领大数据、信息安全产业的发展，应对大数据和信息安全领域更趋日新月异的挑战。